



The Dual Nature of AI; A Double-Edged Sword Amid Digital Transformation; an Ethical Analysis

Ali Talha Khalil¹, Zabta Khan Shinwari^{2*}

1. Department of Pathology, Lady Reading Hospital Medical Teaching Institution, Peshawar, Pakistan.
2. Federal Urdu University of Arts Science and Technology (FUUAST), Pakistan.

Corresponding Author: Zabta Khan Shinwari, Federal Urdu University of Arts Science and Technology (FUUAST), Pakistan. E-mail: Shinwari2008@gmail.com

Received 30 May 2024

Accepted 22 Jun 2024

Online Published 26 Jul 2024

Abstract

Introduction: AI technologies have led to transformative changes in various industries across medicine and healthcare, environmental assessments, smart cities, smart surveillance and security etc. In this article, the dual nature of AI has been investigated.

Material and Methods: It is a review article that described the ethical concerns of societies in AI.

Conclusion: Despite of the many amazing prospective applications, there are ethical and dual use issues of AI which necessitates enhanced governance and vigilance. Addressing these issues requires adherence to the basic ethical principles. Herein, we present the various concerning dimensions of the AI and discuss them under the lens of ethical concepts.

Keywords: *Ethics, Artificial Intelligence (AI), Digital Transformation.*

How to Cite: Talha Khalil A, Shinwari ZK. The dual nature of ai; a double-edged sword amid digital transformation; an ethical analysis, Int J Ethics Soc. 2024;6(2):1-8. doi: [10.22034/ijethics.6.2.1](https://doi.org/10.22034/ijethics.6.2.1)

INTRODUCTION

Recent developments on the interface of Artificial Intelligence (AI) and Internet of Things (IoT) have enabled profound transformations across different research areas in medicine and healthcare, disease surveillance, environmental monitoring, smart cities, urban development, smart gadgets, engineering etc. (1). The fundamental goal of the artificial intelligence (AI) relates to the development of computer-based systems that possess the ability to think, learn and decide as much as the human beings do. In simple words, its relates to the mimicking of human behaviors by the computers (2). It is now recognized that the technological innovation in

the form of artificial intelligence and big data science has the potential to revolutionize the various sectors such as healthcare, academics, etc. by providing robust and reliable ways for data analysis which in other ways are beyond human capabilities. AI has the potential to play a crucial part in the technologies which are defined by theory, method, or approach that assists machines, especially computers, in performing analysis, simulation and exploration of human thought processes and behaviors (3). With enhanced capabilities of problem solving and decision making, it's not far that AI shall reach every field and even every aspect of the human life (4).

Autonomously driving vehicles (AV) are already hovering around with capabilities of making autonomous decisions. The idea of the AV relates to loading the vehicle with many different kinds of sensors which are enabled through AI for fast processing to monitor the surrounding environment of the vehicle and take decisions. The applied sensors within the vehicle enable it to capture thousands of data every millisecond and the use of AI empowers the data to act accordingly in a fast manner. The AI-enabled IoT capabilities in an automobile enable automatic parking, braking, and changing lanes, which is a huge impact on the future of driving (5).

Despite appearing fancy, such technologies have a string of ethical, moral and dual use concerns. For example, in 2016; a Tesla car traveling in autopilot mode crashed and the passenger died (6). The concern is that how it shall be ensured that the decisions these autonomous cars take, will be rendered ethically? and whom to blame for the accident? the passenger? Or the company that makes the car? Autonomous vehicles have privacy and security implications which can undermine the expected benefits if not regulated. These autonomous vehicles can become a new subject for cyber-attacks and hacking and further be controlled for nefarious purposes thus posing a great risk to safety and security (7).

The other prospects in the context of how AI is transforming our lives relates to the open AI's ChatGPT for generative text writing. ChatGPT has the ability generate text for preparation of essays, scholarly manuscripts, presentations etc. In medical fields, AI has exceptional potential for the transformation of the healthcare system and the general principle is to provide computer-based assistance for medical professional for effective treatment, diagnostics etc. Other positives of the AI in health includes enhancing patient-centered care for accurate diagnoses, and further enhancing the workflow and administrative tasks (8). In addition, AI enables

epidemiologists to track and predict the spread of infectious diseases through data from various sources. Further the applications of AI in health can bring smart wearable technologies that can track and keep records of persons heart rate, sleep quality, diabetes management etc (9). Evolving AI tools can foster rapid innovations in the life sciences, including, synthetic biology.

Artificial intelligence has been used in various countries to model their long-term energy needs and further develop AI tools to balance the energy needs with infrastructural requirements. Such examples have already been demonstrated in technology lagging countries such as Ghana (10). In Norway, AI has been used to establish smart self-regulating electric grid which has increased efficiency to several folds (11, 12). Integration of AI in to weather forecasting revealed enhanced success in the prediction of cyclones and other weather patterns (13). AI-integrated farming is now becoming a normal in various countries.

MATERIAL AND METHODS

This is a review article that is written based on existing information that is gathered from books and articles and authors stated their ethical concerns about AI.

DISCUSSION

Ethical and societal concerns

Bias and Discrimination

One of the ethical and societal implications which is brought under the discussion often relates to the application of AI tools in manner that create further discrimination. The AI tools, for training, depends on the provided algorithms and data sets. The concern relates to the fact that the twisted or biased datasets or intentional training the AI systems as such to promote a specific race, sect, religion etc., The bias may be intercalated in the system consciously or sub-consciously. Despite the fact that increasing evidence reveals that the AI is more impartial than commonly

believed, however, the inherent risk is that AI may promote bias and discrimination if not well developed or not well regulated. There is massive potential of discrimination and biasness in AI-enabled hiring, treatment etc. To harness the benefits of AI in recruiting, organizations should exercise careful selection of their programs, promote the adoption of accountable algorithms, and advocate for improvements in racial and gender diversity within high-tech companies (4). Health sector is also vulnerable to discrimination and biases based on AI if not handled properly. Think of a scenario in which an AI model is trained on a dataset which lacks diversity and equal participation. It has been reported in United states that the bulk of the data between 2015-2019 for imaging AI models was only coming for California, New York and Massachusetts with none from 34 “states (14)”. If the data is desired and non-representative of the majority of the population, potential biases and discrimination may emerge. Furthermore, another potential concerning area relates to the predictive policing which might include training models on biased data through which AI incorporated policing might discriminate against specific groups.

Data secrecy and privacy

Algorithms that are used to train the AI models usually require access of large data sets, for example, in case of the healthcare AI, that data may be the patient medical records, which is considered to be highly confidential and private document. As the health records are very important, hackers may target them for data acquisition. Henceforth, maintaining confidentiality of the records is important (15, 16).

Job Displacement

One of the impacts of AI that it shall have in the coming years is its affect on job market, which would include new job opportunities but also replacing others. As AI and automation

technologies continue to advance and be adopted across various sectors, concerns have been raised about their potential to displace jobs and exacerbate income inequality (17). AI technologies are better in executing tasks of repetitive or routine nature enabling incorporation of AI for various automation jobs across the industry. Particular examples can be the virtual assistants and Chatbots for training them to manage customer inquiries, reducing human involvement. In the context of the industry 4.0, which is characterized by the applications of advanced tools for large scale manufacturing, the twining of AI with robotic technologies is considered crucial predictive maintenance, enhanced quality control, collaborative robotics (cobots), and optimized supply chain operations. Through AI, the robots can be empowered to make intelligent decisions and adapt accordingly (18). The major concern here is that automation of tasks through AI would eventually diffuse the narrative of human skills and thus the human services would no longer be required which itself has a string of social and ethical issues. This displacement creates significant challenges for affected individuals, leading to unemployment and income insecurity.

Dual use implications

Despite of having vast potential to have a positive impact on the society, the AI, has been kept under the concept of disruptive technologies i.e., which relates to a technological innovation that can have a disruptive effect (19). Not only there exist an inherent risk of misuse of AI, there are also ethical and social concerns. AI has dual use potential and can be misused for hostile applications directed towards individuals, specific groups, organizations and national security. The dual-use potential of the AI is not a new problem, however, the issue of how AI can be applied for abusive applications have novel vulnerabilities. With the assistance of Deepfake technologies, enabled by AI, can be used to

produce deep fake videos/audios with extraordinary human resemblance and can be used to spread misinformation, manipulation and fraud (20, 21). One of the potential risks of the AI enabled technologies is data poisoning, which relates to the concept of training an AI machine on false and corrupted data for manipulated decisions by the AI system. Other concepts which is known as “adversarial examples” relates to fool the machine learning models (22).

In addition to the existing dangers, the AI based autonomous weapon systems (AWS) represents another area raising severe security and ethical concerns. AWS relies on AI algorithms for independent decision making and if the system became aberrant or poisoned, the system may target the wrong individuals or groups which would result in casualties and human rights violations. In that case, who shall own the responsibility of harm if the humans were not involved in the decision? This also make system more prone to the hacking and unauthorized use (23). Continual assessment of the ever-changing threat landscape is therefore crucial for establishing mechanisms for governance and further develop sophisticated safeguards for cyber-resilience (24).

Ethics of the Responsible use of AI

The integration of AI systems in routine personal and professional discourse and the inherent duality embodied in AI, demands for the responsible and ethical use of AI. The responsible use of AI includes the applications of AI are based on basic ethical principles like fairness, accountability, transparency, beneficence, non-maleficence, justice etc. Governance of AI within the ethical framework shall mitigate the various associated risks and also enable to build public trust for ensuring that the benefits are distributed equitably. Some of the ethical principles for the governance of AI are discussed.

Fairness and Justice

“Fairness” is a basic attribute of social stability and is synonymous with treating every human with respect and justice. In a society, where a certain human or a group of people are treated in un-just manner, causes social unrest and disturbances. Ensuring fairness of Artificial Intelligence (AI) decisions is one of the major challenges for societies, corporates and governments. Algorithm biases and data poisoning consequently fosters unfairness in AI incorporated applications (25). It’s imperative the fairness should be built in and incorporated at every step of the AI life cycle i.e., from design to deployment. From the very initial step, the AI developers must keep in mind the principles of justice i.e., appropriate, equitable and fair treatment regardless of the race, ethnicity, color etc. The developers of AI should keep in mind if their technology may give rise to potential societal disparities (26).

To ensure, the AI based technologies are applied in fair manner, it’s important to have representation of the diverse group with sufficient data from all groups of the affected population for avoiding any discriminatory bias. There are many ways in which can cause bias in the AI decision making, for example, sampling bias can occur due to un-representative sample. Algorithmic bias can occur by training the model on selected attributes or preferences etc. (27). Furthermore, measures should be in place in cases of intentionally injecting fake data for manipulated outcomes. In the context, a “fair AI” is the probabilistic decision support for neutrality and preventing harm or benefits to different groups with an objective to reduce discrimination and quantify bias (28).

Transparency and Explainability

One of the built-in pre-requisites and most emphasized topic covered under the responsible AI is transparency and explainability (29, 30). Transparency in responsible AI relates to making

the decision making of AI, more open, accessible and understandable to everyone. This transparency is indispensable for building confidence among the technology users, decision makers and regulatory bodies. AI models should produce interpretable and human understandable explanations for its decisions. Interpretability in the AI systems should be incorporated without affecting performance (31, 32). For fostering transparency within AI, disclosure of information by the technology developers needed to be increased (33). Open data sharing is considered a pivotal strategy for increasing transparency and reduce bias in AI which relates to the application of diverse sets of data to avoid developing discriminatory algorithms. Open availability of data also ensures enhanced scrutiny by the public and researchers and such initiatives should be embodied in the principles of diversity, inclusion and participation. Despite benefits, however, there exists an inherent trade-off between open data sharing and privacy concerns, henceforth, the risks and benefits need to be weighed. Striking balance is between privacy/security issues and open data sharing shall be the key for responsible AI (34).

Accountability

In general way, the term accountability refers to the state of responsibility and answerability of an action, a behavior, a system, a product, an action etc. In the context of AI, accountability refers to the set of measures, processes, steps that makes AI systems, their developers, users and owners responsible for their actions (35, 36). Accountability issues rise in AI when it produces a result which does not portray the factual circumstances and the AI has changed the fundamental logics of decision-making. Similarly, the AI is usually having the concern of inequitable or disproportionate distribution of risk and harms (37, 38). Various authors define accountability in various different forms in

relation to AI. To some, accountability relates to the explicability, and any AI program, algorithm and outcome, if it can be explained is considered accountable (39).

Accountability in AI however has a dilemma that it's not clear that what should be held accountable for the actions of AI? Whether it's the program developer? Manufacturer or the data supplier, either the producer or manufacturer of the AI system or the supplier of the data. There are multiple views on the accountability of the outcome from AI. Some authors suggest that the AI applications are based on human decisions and they are to be accountable for the actions of AI if needed (40, 41). Yet, there are views from other researchers that the AI and humans are accountable (42).

Privacy

Another concerning question about the application of AI relates to compromising of privacy. The modern AI such as generative AI is being considered to have substantial privacy risks. There have been cases in which AI has been used by the law and enforcement agencies to identify people of unknown identity by matching their photos with the photos that are online available by training a facial recognition model, and similar techniques were applied to identify the protestors in Black Lives Matter (43). In many instances AI technologies have inadvertently revealed the personal data used in their training. In one particular example, a chatbot Lee Luda, trained on real-world text conversations, uncovered the identity of the users whose data were used for training. Generative AI can create similar appearing but fake human faces that illustrates to have the capability of reconstructing the original personal data on which they were trained (44, 45). Under the umbrella of privacy, the AI also has risks of intruding and disturbing the physical space. Not only the AI technologies have the considerable risk in monitoring individual behaviors, patterns but also has a tremendous

potential for the ubiquitous surveillance which has its own set of concerns (43). The risk of identification real time through facial recognition systems is yet another concerning issue related to privacy. For example, a facial recognition model was developed in Italy to prevent entry of already banned individuals from sports in football stadiums, while, the system was also capable of picking up racist conversations (46)

Since for the improvement of AI is largely dependent on the data from different sources to enrich datasets which are used to train models and combined with the coupled with the never-ending demand for data, it's expected that the privacy risks with AI are only going to exacerbated in the real world.

Beneficence and non-maleficence

Beneficence in AI recognizes that AI systems are to be developed to benefit individuals and society at large by strengthening the positive applications and minimizing potential harms. The idea is that the AI should be encourage for achieving common good (47). Beneficence can be promoted in the AI applications thorough respecting diversity, promoting collective approaches. Beneficence and non- non-maleficence though can be considered as sister terms however beneficence differs from non-maleficence in that it involves taking proactive steps to promote the welfare of others, while non-maleficence focuses on avoiding harm (48).

CONCLUSION

The integration of AI in every aspect of human life marks a new beginning. No doubt, AI's ability to mimic human intelligence and making autonomous decisions is driving developments that has the potential to yield several benefits for enhancing data analysis, operational efficiency and decision-making. Despite advantages, AI suffers from an inherent ethical and dual use dilemma and has many social, ethical, moral concerns which necessitate a dire need for the

responsible use of AI and must be addressed. The risks and benefits need to be carefully weighed and concepts of fairness, transparency, diversity, and public trust should be considered. Integration of AI has immense potential but vigilance and commitment to its ethical use is required for a positive impact.

ETHICAL CONSIDERATIONS

Ethical issues (such as plagiarism, conscious satisfaction, misleading, making and or forging data, publishing or sending to two places, redundancy and etc.) have been fully considered by the writers.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interests.

REFERENCES

1. Bibri S E, Krogstie J, et al. Smarter eco-cities and their leading-edge artificial intelligence of things solutions for environmental sustainability: A comprehensive systematic review. *Environmental Science and Ecotechnology*, 2024; 19(16): 100330. Doi: [10.1016/j.ese.2023.100330](https://doi.org/10.1016/j.ese.2023.100330)
2. De Haro L P. Biosecurity risk assessment for the use of artificial intelligence in synthetic biology. *Applied Biosafety*, 2024; 29(2). Doi: <https://doi.org/10.1089/apb.2023.0031>
3. Lu Y. Artificial intelligence: a survey on evolution, models, applications and future trends." *Journal of Management Analytics*, 2019; 6(1): 1-29. Doi: [10.1080/23270012.2019.1570365](https://doi.org/10.1080/23270012.2019.1570365)
4. Chen Z. Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanities and Social Sciences Communications*, 2023; 10(1): 1-12. Doi: [10.1057/s41599-023-02079-x](https://doi.org/10.1057/s41599-023-02079-x)
5. Abed A K, Anupam A. Review of security issues in internet of things and artificial intelligence-driven solutions. *Security and Privacy*, 2023; 6(3): e285. Doi: [10.1002/spy2.285](https://doi.org/10.1002/spy2.285)
6. Levin S, Woolf N. Tesla driver killed while using autopilot was watching Harry Potter, witness says. *The Guardian* 2016. [Accessed 21 May 2024]. Available at: <https://www.theguardian.com/technology/2016/jul/01/tesla-driver-killed-autopilot-self-driving-car-harry-potter>
7. Bendiab G, Hameurlaine A, et al. Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence. *IEEE Transactions on Intelligent Transportation Systems*, 2023; 24(4): 3614-3637. Doi: [10.1109/TITS.2023.3236274](https://doi.org/10.1109/TITS.2023.3236274)
8. Rigby M. Ethical dimensions of using artificial intelligence in health care. *AMA J Ethics*. 2019; 21(2): 121–124. Doi: [10.1001/amajethics.2019.121](https://doi.org/10.1001/amajethics.2019.121)
9. Benkaddour M K, Bendehiba K. et al. Efficient image classification for early prediction of Alzheimer's disease. Master thesis. Kasdi Marbah University Ouargla; 2023.

10. Byrne D. (2024). "How artificial intelligence is helping Ghana plan for a renewable energy future. Nature Career Podcast, 2024; Available at: <https://www.nature.com/articles/d41586-024-01316-w>
11. Kurbatsky V, Tomin N. Smart system of monitoring and forecasting for electric power systems. IEEE International Conference on Power System Technology (POWERCON), 2012. Doi: [10.1109/PowerCon.2012.6401289](https://doi.org/10.1109/PowerCon.2012.6401289)
12. Schiavo L L, Delfanti M, et al. Changing the regulation for regulating the change: Innovation-driven regulatory developments for smart grids, smart metering and e-mobility in Italy. Energy Policy, 2013; 57: 506-517. Doi: <https://doi.org/10.1016/j.enpol.2013.02.022>
13. Lopatka A. Meteorologists predict better weather forecasting with AI. Physics Today, 2019; 72(5): 32-34. Doi: [10.1063/PT.3.4201](https://doi.org/10.1063/PT.3.4201)
14. Kaushal A, Altman R, et al. Geographic distribution of US cohorts used to train deep learning algorithms. The Journal of the American Medical Association, 2020; 324(12): 1212-1213. Doi: [10.1001/jama.2020.12067](https://doi.org/10.1001/jama.2020.12067)
15. Murdoch B. Privacy and artificial intelligence: challenges for protecting health information in a new era. BMC Medical Ethics, 2021; 22(1): 1-5. Doi: [10.1186/s12910-021-00687-3](https://doi.org/10.1186/s12910-021-00687-3)
16. Khan B, Fatima H, et al. Drawbacks of artificial intelligence and their potential solutions in the healthcare sector. Biomedical Materials & Devices, 2023; 1(2): 731-738. Doi: [10.1007/s44174-023-00063-2](https://doi.org/10.1007/s44174-023-00063-2)
17. Du J. The impact of artificial intelligence adoption on employee unemployment: A multifaceted relationship." International Journal of Social Sciences and Public Administration, 2024; 2(3): 321-327. Doi: [10.62051/ijsspa.v2n3.45](https://doi.org/10.62051/ijsspa.v2n3.45)
18. Mia M R, Shuford J. Exploring the Synergy of Artificial Intelligence and Robotics in Industry 4.0 Applications. Journal of Artificial Intelligence General science (JAIGS), 2024; 1(1). Doi: [10.60087/jaigs.v1i1.31](https://doi.org/10.60087/jaigs.v1i1.31)
19. Páváloaia VD, Necula S C. Artificial intelligence as a disruptive technology—a systematic literature review. Electronics, 2023; 12(5): 1102. Doi: <https://doi.org/10.3390/electronics12051102>
20. Jones V A. Artificial intelligence enabled deepfake technology: The emergence of a new threat. Ph.D. thesis. University of Utica, New York; 2020.
21. Okolie C. Artificial intelligence-altered videos (deepfakes), image-based sexual abuse, and data privacy concerns. Journal of International Women's Studies, 2023; 25(2): 13.
22. Goodfellow I J, Shlens J, et al. Explaining and harnessing adversarial examples. International Conference on learning Representations, 2014; Corpus ID: 6706414
23. Rashid A B, Kausik A K, et al. Artificial intelligence in the military: An overview of the capabilities, applications, and challenges. International Journal of Intelligent Systems, 2023; 4: 1-31. Doi: [10.1155/2023/8676366](https://doi.org/10.1155/2023/8676366)
24. Blauth T F, Gstrein O J, et al. Artificial intelligence crime: An overview of malicious use and abuse of AI. IEEE Access, 2022; 10: 77110-77122. Doi: [10.1109/ACCESS.2022.3191790](https://doi.org/10.1109/ACCESS.2022.3191790)
25. Larson J, Mattu S, et al. How we analyzed the COMPAS recidivism algorithm. ProPublica, 2016; 9(1).
26. Morgan M B, Mates J L. Ethics of artificial intelligence in breast imaging." Journal of Breast Imaging, 2023; 5(2): 195-200. Doi: [10.1093/jbim/wbac076](https://doi.org/10.1093/jbim/wbac076)
27. Ferrara E. Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies. Sci, 2023; 6(1): 3. Doi: <https://doi.org/10.3390/sci6010003>
28. Barocas S, Selbst A D. Big data's disparate impact. Calif. L. Rev. 2016; 104: 671. Doi: <https://doi.org/10.2139/SSRN.2477899>
29. Cysneiros L M, Raffi M, et al. Software transparency as a key requirement for self-driving cars. IEEE 26th International Requirements Engineering Conference (RE), 2018; Doi: [10.1109/RE.2018.00-21](https://doi.org/10.1109/RE.2018.00-21)
30. Chazette L, Brunotte W, et al. Exploring explainability: a definition, a model, and a knowledge catalogue. IEEE 29th International Requirements Engineering Conference (RE), 2021.
31. Lodge M. Accountability and transparency in regulation: critiques, doctrines and instruments. 1st ed. Cheltenham/United Kingdom: Edward Elgar Publishing. 2004.
32. Ras G, Xie N, et al. Explainable deep learning: A field guide for the uninitiated. Journal of Artificial Intelligence Research, 2022; 73: 329-396. Doi: [10.1613/jair.1.13200](https://doi.org/10.1613/jair.1.13200)
33. Jobin A, Ienca M, et al. The global landscape of AI ethics guidelines. Nature Machine Intelligence, 2019; 1(9): 389-399. Doi: [10.1038/s42256-019-0088-2](https://doi.org/10.1038/s42256-019-0088-2)
34. Akinrinola O, Okoye C C, et al. Navigating and reviewing ethical dilemmas in AI development: Strategies for transparency, fairness, and accountability. GSC Advanced Research and Reviews, 2024; 18(3): 50-58. Doi: [10.30574/gscarr.2024.18.3.0088](https://doi.org/10.30574/gscarr.2024.18.3.0088)
35. Memarian B, Doleck T. Fairness, Accountability, Transparency, and Ethics (FATE) in Artificial Intelligence (AI), and higher education: A systematic review. Computers and Education: Artificial Intelligence, 2023; 5(4). Doi: [10.1016/j.caeai.2023.100152](https://doi.org/10.1016/j.caeai.2023.100152)
36. Novelli C, Taddeo M, et al. Accountability in artificial intelligence: what it is and how it works. Ai & Society, 2023; 1-12. Doi: <https://doi.org/10.1007/s00146-023-01635-y>
37. Raji I D, Smart A, et al. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. Conference on Fairness, Accountability, and Transparency, 2020; Doi: [10.1145/3351095.3372873](https://doi.org/10.1145/3351095.3372873)
38. Slota S C, Fleischmann K R, et al. Many hands make many fingers to point: challenges in creating accountable AI. Ai & Society, 2021; 38(9):1-13. Doi: [10.1007/s00146-021-01302-0](https://doi.org/10.1007/s00146-021-01302-0)
39. Bezuidenhout L, Ratti E. What does it mean to embed ethics in data science? An integrative approach based on micro ethics and virtues. Ai & Society, 2021; 36(3): 939-953. Doi: [10.1007/s00146-020-01112-w](https://doi.org/10.1007/s00146-020-01112-w)
40. Pagallo U. From automation to autonomous systems: A legal phenomenology with problems of accountability. 26th International Joint Conference on Artificial Intelligence, 2017; Doi: [10.24963/ijcai.2017/3](https://doi.org/10.24963/ijcai.2017/3)
41. Kong S C, Cheung W M Y, et al. Evaluating an artificial intelligence literacy program for developing university students' conceptual understanding, literacy, empowerment and ethical awareness. Educational Technology & Society, 2023; 26(1): 16-30
42. Li C, Xing W, et al. Using fair AI to predict students' math learning outcomes in an online platform. Interactive Learning Environments, 2024; 32(3): 1117-1136
43. Lee H P, Yang Y J, et al. Deepfakes, phrenology, surveillance, and more! a taxonomy of ai privacy risks. Proceedings of the CHI Conference on Human Factors in Computing Systems, 2024; Doi: <https://doi.org/10.48550/arXiv.2310.07879>
44. Jang H. A South Korean chatbot shows just how sloppy tech companies can be with user data. [Accessed in 21 May 2024]. Available at: <https://slate.com/technology/2021/04/scatterlab-lee-luda->

- [chatbot-kakaotalk-ai-privacy.html](https://doi.org/10.48550/arXiv.2107.06018)
45. Webster R, Rabin J, et al. (2021). This person (probably) exists. identity membership attacks against GAN generated faces. Computer Vision and Pattern Recognition, 2021; 4(2). Doi: <https://doi.org/10.48550/arXiv.2107.06018>
46. Niu J, Liu P, et al. A survey on membership inference attacks and defenses in machine learning. Journal of Information and Intelligence, 2024; (In Press). Doi: <https://doi.org/10.1016/j.jiixd.2024.02.001>
47. Currie G, Hawk K E, et al. Ethical principles for the application of artificial intelligence (AI) in nuclear medicine. European Journal of Nuclear Medicine and Molecular Imaging, 2020; 47: 748-752. Doi: <https://doi.org/10.1007/s00259-020-04678-1>
48. Beauchamp T L, Childress J F. Principles of biomedical ethics. 1st ed. USA: Oxford University Press. 2001.

